INTERNATIONAL JOURNAL OF CRITICAL INFRASTRUCTURE PROTECTION 25 (2019) 125–138

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/IJCIP

Complex approach to assessing resilience of critical infrastructure elements

David Rehak[a,*], *Pavel Senovsky*[a], *Martin Hromada*[b], *Tomas Lovecek*[c]

[a] *Faculty of Safety Engineering, VSB – Technical University of Ostrava, Lumirova 13, 700 30 Ostrava, Czech Republic*
[b] *Faculty of Applied Informatics, Tomas Bata University in Zlin, Czech Republic*
[c] *Faculty of Security Engineering, University of Zilina, Slovak Republic*

ARTICLE INFO

Article history:
Received 29 November 2018
Revised 9 January 2019
Accepted 25 March 2019
Available online 29 March 2019

Keywords:
Critical infrastructure
Resilience assessment
Robustness
Recoverability
Adaptability
Elements

ABSTRACT

The resilience of elements in a critical infrastructure system is a major factor determining the reliability of services and commodities provided by the critical infrastructure system to society. Resilience can be viewed as a quality which reduces the vulnerability of an element, absorbs the effects of disruptive events, enhances the element's ability to respond and recover, and facilitates its adaptation to disruptive events similar to those encountered in the past. In this respect, resilience assessment plays an important role in ensuring the security and reliability of not only these elements alone, but also of the system as a whole. The paper introduces the CIERA methodology designed for Critical Infrastructure Elements Resilience Assessment. The principle of this method is the statistical assessment of the level of resilience of critical infrastructure elements, involving a complex evaluation of their robustness, their ability to recover functionality after the occurrence of a disruptive event and their capacity to adapt to previous disruptive events. The complex approach thus includes both the assessment of technical and organizational resilience, as well as the identification of weak points in order to strengthen resilience. An example of the application of the CIERA method is presented in the form of a case study focused on assessing the resilience of a selected element of electrical energy infrastructure.

© 2019 The Authors. Published by Elsevier B.V.
This is an open access article under the CC BY-NC-ND license.
(http://creativecommons.org/licenses/by-nc-nd/4.0/)

1. Introduction

The functioning of a modern society is based on the extensive use of infrastructure which ensures the basic function of the state from the perspectives of both governance (state and territorial) and the infrastructure providing goods and services (supply, transport, electric power, communications, etc.). Although the significance of these infrastructures has long been known, they began to be researched in a more complex way relatively recently. The term "critical infrastructure" (CI), which these infrastructures have come to be identified with, did not come into more extensive use until the publication of the Critical Foundations study [1].

Each state determines which infrastructure elements (sectors) are included from the complete list of infrastructure elements (sectors) in its critical list. A comparison of critical infrastructure sectors of the European Union Member States was published, for example, in the ENISA study [2]. In individual sectors and sub-sectors, the states then determine the national critical infrastructure elements, whose operation is governed by the relevant legislation – in the Czech Republic, for example, the Crisis Management Act [3]. In this context,

* Corresponding author.
E-mail address: david.rehak@vsb.cz (D. Rehak).

https://doi.org/10.1016/j.ijcip.2019.03.003
1874-5482/© 2019 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license.
(http://creativecommons.org/licenses/by-nc-nd/4.0/)

critical infrastructure can be understood as a comprehensive system and individual sectors and sub-sectors as its subsystems, which are made up of individual elements. These elements may be of a structural or equipment nature.

It is imperative that these infrastructures maintain a high level of reliability and security. Consequently, such system infrastructures should be highly resilient to the effects of both internal and external threats. Resilience in the context of critical infrastructure was first defined in 2009 as "*the ability to absorb, adapt to, and/or rapidly recover from a potentially disruptive event*" [4]. However, in developing CI resilience, emphasis was increasingly placed on the adaptation of critical infrastructure to changing conditions over time [5].

In the intervening period, the system of critical infrastructure underwent extensive research with respect to the assessment of its resilience. The first comprehensive study defining the components of critical infrastructure resilience was the Resilience Measurement Index [6]. It classifies these components in four basic groups: Preparedness, Mitigation Measures, Response Capabilities and Recovery Mechanisms. However, this classification is not complete in that it fails to address adaptability as the ability of a critical infrastructure subsystem to adapt to disruptive events similar to those it had encountered in the past.

The Measuring Critical Infrastructure Resilience study [7] presents possible indicators of resilience but does not provide any procedure for its evaluation. The first evaluation concept was introduced as part of the Guidelines for Critical Infrastructure Resilience Evaluation [8]. Evaluation in line with these guidelines is framed in four dimensions: logical and physical (technical), personal, organizational and cooperative.

In recent years, a number of studies have been published presenting various methodical approaches to evaluating critical infrastructure resilience (e.g., [9–11]). While these publications brought numerous new findings as regards resilience quantification, their approach to the issue was mostly system-based [12]. Evaluation thus focused primarily on the system or sector level of critical infrastructure [13], altogether omitting the elementary level. In fact, this level of critical infrastructure should not be ignored because it is at the level of elements that protective measures, or measures aimed at strengthening resilience, are often implemented. A complex evaluation of infrastructure elements can provide valuable feedback to help identify weak points. Such information can then act as support in deciding the allocation of resources to initiate activities for the purpose of strengthening resilience. For example, Labaka et al. [14] argues for the need to modify crisis management as the tool for responding to unexpected events, as distinct from the Government of Canada [15], which bases its action plan on risk management. Both approaches, however, employ resilience as the means by which to achieve these objectives. Therefore, management in its various forms can be said to perform an integral role in ensuring the functions and protection of critical infrastructure.

The technical aspects of resilience have been studied, for example, by Dueñas-Osorio et al. [16], who examined the fragility of network infrastructure in terms of its ability to withstand seismic activity. Several studies also focus on the interdependence of elements in critical infrastructure networks and their fragility (e.g., [17–19]). However, these approaches focus on the critical infrastructure network as a whole. Such information is useful for strategic network management but does not provide the information needed to implement safeguards at the element level.

In the context of the above, was launched in 2015 the research project of the Ministry of the Interior of the Czech Republic, entitled "RESILIENCE 2015: Dynamic Resilience Evaluation of Interrelated Critical Infrastructure Subsystems", which focuses on the dynamic evaluation of critical infrastructure sectors, namely the electricity, transport and ICT sectors. One of the main goals of the project was to develop effective methods for evaluating the resilience of individual elements of critical infrastructure.

Element resilience is the factor determining the resilience of higher critical infrastructure subsystems formed by these elements. This led the authors to develop the CIERA method (Critical Infrastructure Elements Resilience Assessment), which primarily focuses on equipment evaluation, as part of the above-mentioned project. The method and its components, procedures and methodologies are presented in more detail below. Its basic premises have already been published recently in the paper entitled Resilience of Critical Infrastructure Elements and its Main Factors [20].

2. Basic premises of resilience assessment in a critical infrastructure system

The term resilience was first defined in 1973 by Holling [21] as the ability of a system to absorb or resist the effects of failures and other stress factors without any changes to the functioning of the system. Although this wording was first applied to ecological systems, over time the term resilience began to appear in other scientific fields, including sociology, psychology and economics. The relatively youngest field, with respect to system resilience research, is engineering.

However, each of these fields views resilience somewhat differently. While ecology employs resilience as a tool to learn more about the dynamics of an ecological system's response to external or internal impulses that disrupt its functionality, in anthropogenic systems (such as critical infrastructure systems or communities) resilience is regarded more as the desirable target status [20]. Society in general expects these systems to be highly resilient.

Whereas ecosystem resilience is, to a certain extent, formed autonomously, the resilience of anthropogenic systems, as the desirable target status, must be developed and strengthened artificially. That is why the existing risk management systems are not sufficient to strengthen resilience, as they fail to cover the entire spectrum of resilience. Resilience essentially provides a much broader view of the issue of safety – it contains both processing and technical components.

2.1. *Cycle of critical infrastructure resilience*

Resilience is one of the key factors contributing to the preservation of the functionality of critical infrastructure subsystems, i.e. sectors, subsectors and elements [13]. It represents

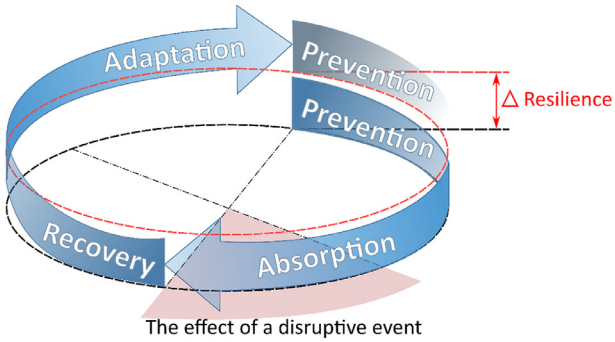

Fig. 1 – Critical infrastructure resilience cycle [23].

the ability of these subsystems to mitigate the intensity of impacts caused by a disruptive event and to reduce the duration of their failure or disruption [22]. From this perspective, resilience is a major factor determining the reliability of critical infrastructure subsystems and may be understood as a cyclic process based on the continual enhancement of system prevention, absorption, recovery and adaptation [23]. Fig. 1 shows one cycle within which resilience is strengthened from its original level (i.e. the black dashed line) to a new one (i.e. the red dashed line). The difference between these two levels Δ is understood as the degree to which resilience has been strengthened.

The initial phase of the resilience cycle is prevention, whereby subsystems are continually prepared for future disruptive events. Absorption, the second phase of the resilience cycle, is determined by the robustness of critical infrastructure subsystems and involves the ability of subsystems to absorb the effects of these events without them causing fluctuations in the provision of services. The recovery phase starts after the effects of a disruptive event have worn off and is characterized by recoverability, which is the capacity of a subsystem to recover its function to the required level of performance. The final phase of the resilience cycle is adaptation, which is essentially the ability of an organization to adapt utilized subsystems to the potential recurrence of disruptive events.

2.2. *Framework for assessing the resilience of critical infrastructure elements*

The assessment of the resilience of critical infrastructure elements is a specific and professionally demanding process. Some basic principles, including the principles of complexity, specificity, adequacy, impartiality and expertise, should therefore be applied in its implementation [24]. Moreover, the assessment process should be based on clearly defined procedures and quantitative supporting data.

For the purposes of assessing CI resilience, the research team focused primarily on the basic structural and performance parameters of the element concerned, the existing safety measures of the element being assessed, the organizational processes supporting the strengthening of element resilience and, last but not least, specific disruptive events against which the element's resilience is to be assessed (see Fig. 2).

The assessment involves elements which the organization identified as of interest. The structural and performance parameters mainly represent the internal arrangement of these elements within the critical infrastructure system as a whole. From a structural point of view, they can have the character of point elements, line elements or areal elements (i.e. a point element including two or more key technologies). Performance parameters then refer especially to the quantity and performance of key technologies.

The current level of resilience is determined by the existing (already adopted) safety measures within the context of assessments focused primarily on element robustness and recoverability. This requires current knowledge of the level of crisis preparedness, redundancy, detection capability, responsiveness, physical resistance (i.e. technical means and organizational or system measures), as well as material, financial and human resources or processes required for element recovery following a disruptive event.

Organizational processes are another important source of supporting data which helps form the resilience assessment framework. Good knowledge thereof allows assessment of the level of adaptability of the element to previous disruptive events. The processes of risk management, innovation, education and development are of particular interest in this context.

Since resilience assessment can only be carried out with regard to specific disruptive event scenarios, it is essential that we proceed based on threats which the element being assessed may be exposed to. The method includes eight basic threat groups to facilitate the process of assessment (see Table 1). In selecting individual groups, the team relied on the PERIL disaster event classification used in databases of large-scale event consequences [25]. From these events, the team selected groups wherein threats primarily concern infrastructure.

For the purposes of assessment, the threats have been classified as internal and external. The further division into naturogenic, technogenic and anthropogenic causes is based on the general nature of each threat. However, the PERIL framework [25] takes into account only technological threats. In order to carry out the assessment of critical infrastructure resilience it was necessary to differentiate between threats arising from mere technological failures and those caused directly by humans (e.g. sabotage or terrorist attacks). The group of cascading effects was added to allow for the capturing of failure propagation across the critical infrastructure system via cascading effects [26].

The classification of threats given above is only general in nature and the operators of critical infrastructure elements can modify it to better reflect the character of threats to which their particular elements are exposed.

2.3. *Components and variables determining the resilience of critical infrastructure elements*

The initial stage in preparing the CIERA method involved a comparative analysis of the relevant papers published to date. The results were used to propose the structural components and some variables. This structure is primarily based on the critical infrastructure resilience final report and

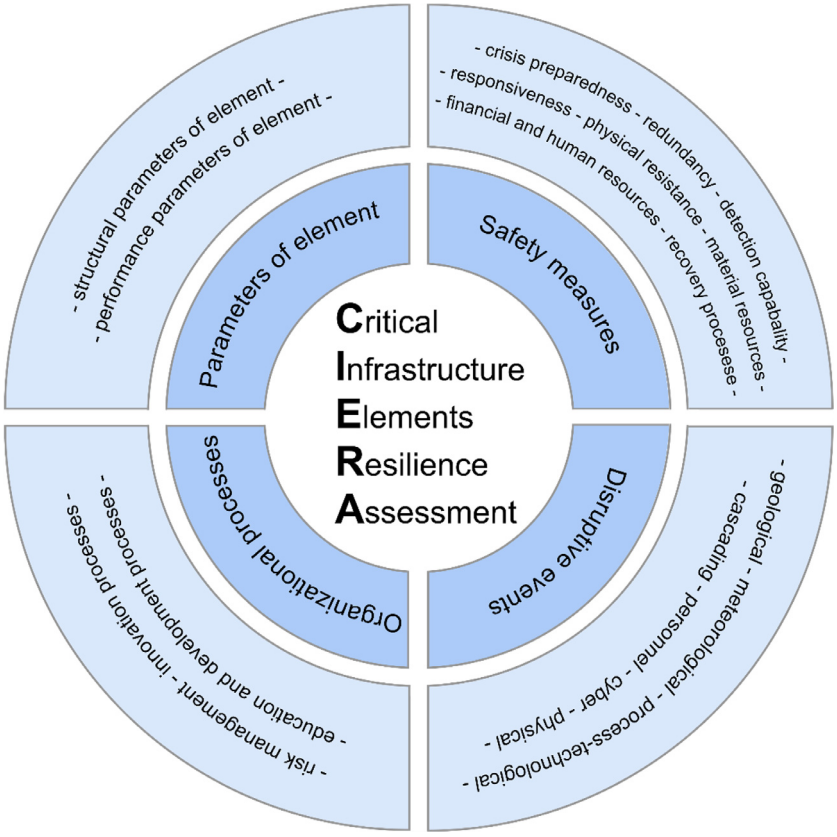

Fig. 2 – Framework for assessing the resilience of critical infrastructure elements.

Table 1 – Classification of threats for assessing the resilience of critical infrastructure elements.

	Naturogenic	Technogenic	Anthropogenic
Internal threats	–	Process-technological threats	Personnel threats
External threats	Geological threats	Cascading threats	Cyber threats
	Meteorological threats		Physical threats

recommendations document [4]; however, it also partially reflects two other important studies published in 2012 [27,28]. The subsequent phase consisted of defining any potentially measurable items. The definition of these items was based on publications addressing issues related to resilience measurement indicators [6–8].

Based on the available data, the authors of the method proceeded to formulate individual determining factors of resilience. This preparation stage hinged on the implementation of all variables determining all phases of resilience, i.e. prevention, absorption, recoverability and adaptability. The definition of these determinants was limited by some factors that stem from the focus of the project. Therefore, the assessment components are primarily focused on individual critical infrastructure elements, as opposed to the sector or subsector as a whole. The selection was also influenced by the planned utilization of the results as the basis for the long-term management of element resilience. Accordingly, the assessment is principally focused on the issue of management.

This stage resulted in the specification of 12 variables and 167 measurable items being discussed with selected operators and owners of critical infrastructure elements at the project workshop held at the beginning of 2017. The variables and measurable items were subsequently classified into two basic areas, namely (1) technological and physical protection of elements and (2) organization management.

Resilience in the first area, referred to as technical resilience, is determined by the robustness and recoverability of infrastructure elements. The enhancement of technical resilience is invariably achieved exclusively in relation to a particular element or group of identical or very similar elements. A good example is the electricity sector, where robustness and recoverability will be secured in different ways and by different means depending on whether we are dealing with systems for the production of electricity or systems employed for its transmission and distribution.

The second area constituting element resilience is organization management. This type of resilience, known

Table 2 – Areas, components and variables determining the resilience of critical infrastructure elements.

Areas	Technical resilience		Organizational resilience
Components	Robustness	Recoverability	Adaptability
Variables	Crisis preparedness Redundancy Detection capability Responsiveness Physical resistance	Material resources Financial resources Human resources Recovery processes	Risk management Innovation processes Education and development processes

as organizational resilience, is determined by the level of an organization's selected internal processes focused on the creation of optimum conditions for the adaptation of critical infrastructure elements to disruptive events. Organizational resilience is formed simultaneously for all critical infrastructure elements operated by an organization.

For variables determining the individual components of the resilience of critical infrastructure elements see Table 2.

Robustness is the ability of an element to absorb the impacts of a disruptive event. These impacts may be absorbed via the structural qualities of buildings or the technologies used (i.e. structural robustness) and/or via security measures (i.e. security robustness). The level of robustness can only be assessed relative to a particular disruptive event or, rather, the intensity thereof. Where this level reaches 100%, the element concerned becomes resistant to the impacts of the given disruptive event. This means that it is able to fully resist its effects without perceptible negative impacts on the element of the service provided.

Recoverability is the capacity of an element to recover its function to the original (required) level of performance after the effects of a disruptive event have ended. With respect to critical infrastructure, recoverability is understood as reparability, in which case only the damaged or destroyed components of an element are repaired or replaced. Provided the recoverability (see the variables listed in Table 2) resources are adequate, resilience can already be strengthened at this stage. The implementation of more modern technologies, meeting higher security standards and ensuring greater element robustness, can be used as an example.

Adaptability is the ability of a critical infrastructure operator (i.e. an organization) to prepare an element for the potential effects of disruptive events similar to those that occurred in the past. Furthermore, it represents the dynamic (long-term) ability of an organization to adapt to changes in circumstances.

In the context given above, individual components and variables determining resilience can be said to affect the dynamics of the performance of the services provided by an element in response to a disruptive event (see Fig. 3). This dynamic can vary depending on the type of infrastructure and the disruptive event and the manner of its management.

As soon as an element begins to be affected by a disruptive event, the absorption capacity of the element can be broken down into two phases. In the first phase, the system is able to absorb the impacts of a disruptive event without the need to employ redundant capacities, up to the boundary of the element's ability to absorb fully the impacts of the respective disruptive event (see point A in Fig. 3). In the second phase of absorption, the redundant capacities available to the element are employed and the element is still capable of delivering its full performance as required. At this point, there is still an opportunity to detect adverse events and initiate a suitable response [20].

Only after the redundant capacities of the element have been exhausted, i.e. the limit of its ability to absorb the impacts of a disruptive event has been reached (see point B in Fig. 3), do the negative consequences of the event begin to manifest in a decline of functions performed by the element. The nature of this decline is determined by the capabilities of the element to defend against the effects of the event. Where such capabilities exist, the decline in performance of the element may be gradual; however, if these capabilities are overcome by the intensity of the disruptive event, the decline is likely to be abrupt or even immediate [20].

3. Assessing the resilience of critical infrastructure elements

The CIERA method was created to assess the resilience of critical infrastructure elements. This method was developed as part of the grant project of the Ministry of the Interior of the Czech Republic entitled "RESILIENCE 2015: Dynamic Resilience Evaluation of Interrelated Critical Infrastructure Subsystems". It was designed for the assessment of element resilience in technically oriented sectors such as energy, water management, transport and communication/information systems. However, the manner of assessment and some of the metrics, when modified, can also be applied to other sectors; for example, to evaluate the resilience of elements in the emergency services or health sectors.

As the proposed CIERA method focuses on assessing the resilience of elements without the possibility of factoring in the network characteristics of critical infrastructure, the following limiting conditions have been set for its application:

- The assessment focuses on individual/specific elements of critical infrastructure. The subject of the assessment is the internal ability of critical infrastructure elements to counter the effects of both internal and external disruptive events.
- The assessment must always be aimed at a particular disruptive event.
- The created resilience model is static – the assessment takes place in the phase of zero intensity with respect to

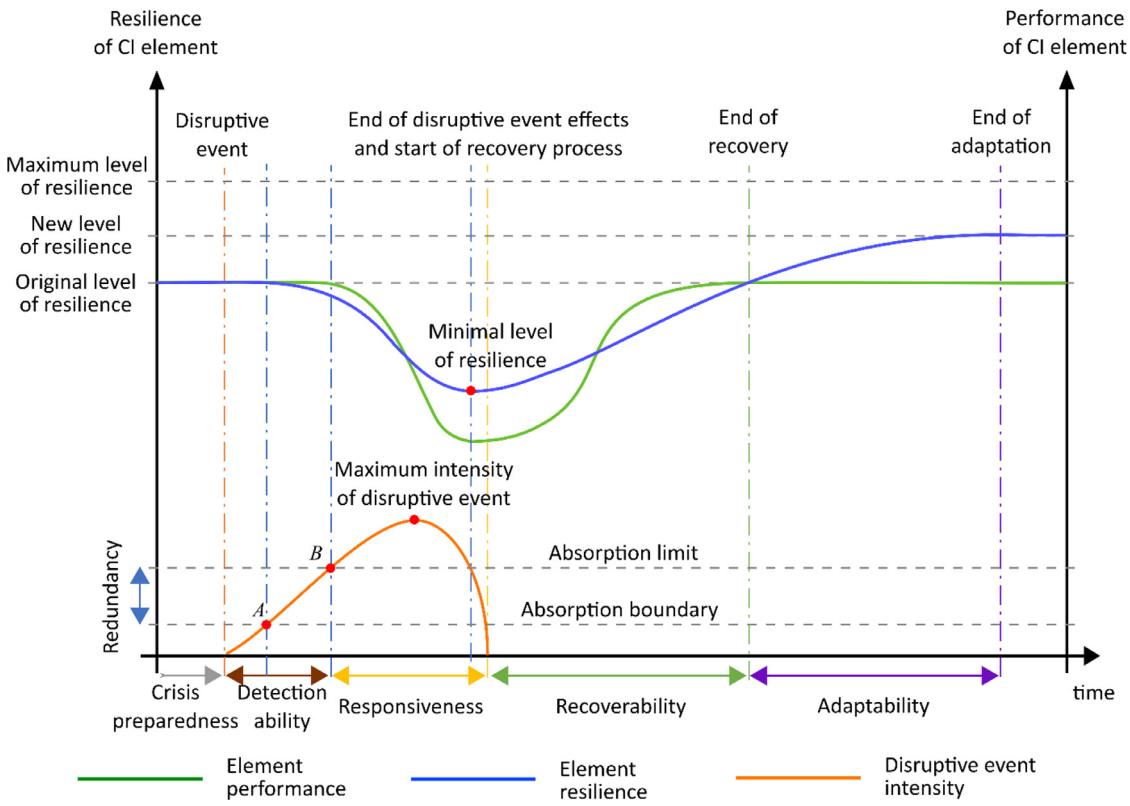

Fig. 3 – Graphical representation of components and variables determining the resilience of critical infrastructure elements [20].

the disruptive event, i.e. at a point where the event is not affecting the critical infrastructure element.

3.1. *Resilience assessment procedure*

The crucial phase of the CIERA method creation involved the establishment of the resilience assessment procedure. This procedure is based not only on general methods (e.g. [29]), but it also incorporates features from specific methodologies (e.g. [9–11]).

The procedure for assessing the resilience of critical infrastructure elements includes nine consecutive activities. These activities consist of selecting and describing the element being assessed, identifying and describing the threats against which the element is to be assessed, assessing the level of individual components that determine the element's resilience, calculating the element's resilience, evaluating the weak points and proposing measures aimed at strengthening the element's resilience. The sequence of individual activities is shown in Fig. 4 below.

There are no restrictions as to the selection of an element (*Activity 1*). In developing the method, the research team focused primarily on technical sectors. The method was tested on designated elements of the electricity (see Section 4 herein), transport and health sectors. However, the team presumes the possibility of a wider application of the method's principles.

Subsequently the selected element is described (*Activity 2*) as to its structural and performance parameters and categorized within the structure of the critical infrastructure. Element categorization is based on the sector, subsector or any other structural specification (e.g. production, transmission or distribution with regard to the electricity sector) within which it was first determined on the basis of sectoral criteria. Conversely, the performance parameters specify the element's technological structure, which highlights the number and capacity of key technologies.

For the purposes of the assessment, it is necessary to identify (*Activity 3*), classify and describe all threats (*Activity 4*) which have the potential to initiate disruptive events leading to a major decline or even interruption in the provision of services. The assessment should be conducted separately for each identified threat. Scenarios describing the progress of such events could be utilized as an appropriate supporting tool. In addition, these scenarios could also be viewed as a by-product of the proposed method; applicable, for example, to the dynamic modeling of resilience, reflecting the course of the disruptive event's intensity; or to the modeling of cascading and synergistic effects within a critical infrastructure system (for example [13,30,31]). Activities 1 and 2 must be done sequentially. Similar approach should be done with activities 3 and 4. However, both sequences (i.e., 1, 2 and 3, 4) could be solved at the same time.

The assessment of robustness (*Activity 5*) hinges on assessing the element's ability to absorb the impacts of disruptive

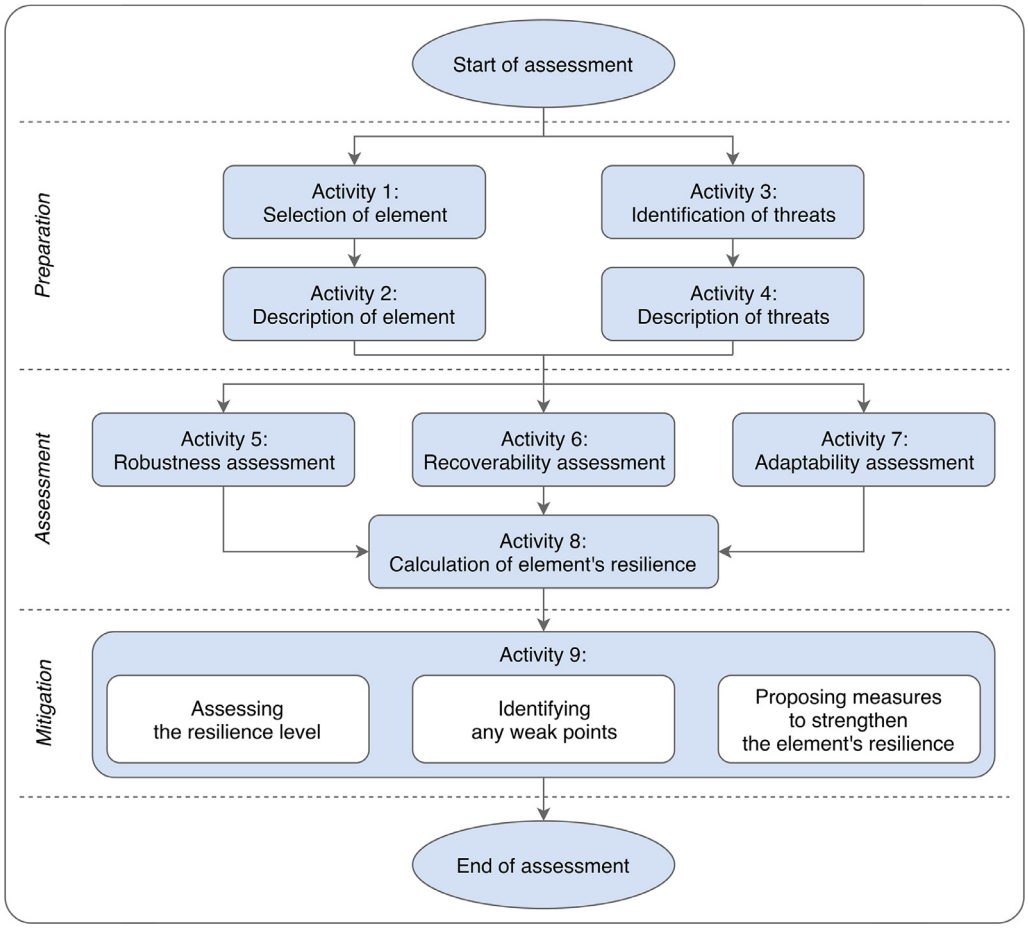

Fig. 4 – Procedure for assessing the resilience of critical infrastructure elements.

events. The level of all measurable items which determine a variable must be assessed for each of the variables. The assessment is based on a scale from 1 (worst) to 5 (best). For example, the measurable item "Activation speed of substitution linkages" is assessed on the following scale:

5: Immediate activation (no reduction in performance).
4: Delayed activation causing a short-term reduction in performance of the assessed element.
3: Delayed activation causing a short-term loss of performance of the assessed element.
2: Delayed activation causing a medium-term loss of performance of the assessed element.
1: Delayed activation causing a long-term loss of performance of the assessed element.

Element robustness is to be assessed with respect to a selected particular threat. Based on this, one of the assessment forms is used for the assessment. Assessments of recoverability (*Activity 6*) and adaptability (*Activity 7*) are carried out similarly. Each assessment activity has its own measurable items with a specific assessment scale.

The core activity of the procedure is the calculation of the element's resilience (*Activity 8*). For the purposes of this method, we have opted for a quantitative assessment model. This model is based on the percentage expression of the degree of fulfillment of individual components determining the element's resilience. This type of expression already includes comparative values and can be readily used in other applications; for example, in the modeling of cascading and synergistic effects within a critical infrastructure system (see [13,30,31]).

The resilience level of the critical infrastructure element is calculated as the arithmetic mean of the component values that determine it (Formula (1)):

$$R = \frac{1}{n}\sum_{i=1}^{n} K_i \tag{1}$$

where R = the resilience of the critical infrastructure element [%]; K = the resilience components of the critical infrastructure element, i.e. robustness, recoverability and adaptability [%]; n = the total number of components determining resilience. For a possible graphical representation of the critical infrastructure element's level of resilience, see Fig. 5.

The levels of individual components of the CI element's resilience are determined by the weighted average of its variables (Formula (2)):

$$K_i = \sum_{j=1}^{m} P_j v_j \tag{2}$$

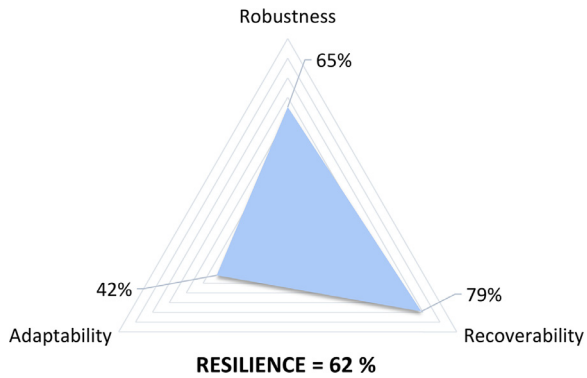

Fig. 5 – The resilience level of the critical infrastructure element.

where K_i = the ith component of the critical infrastructure element's resilience [%]; P_j = the jth variable of the critical infrastructure element's resilience [%]; v_j = the jth normalized weight of the jth variable of the critical infrastructure element's resilience [⟨0; 1⟩]; m = the total number of variables in the ith component. The normalized weights of the variable are presented in the following part of the paper.

For a possible graphical representation of the level of the selected resilience component of the critical infrastructure element and its variables, see Fig. 6.

The levels of the resilience variables of the critical infrastructure element are determined by the weighted average of individual measurable items (Formula (3)). Since the level of measurable items is expressed on a point scale in intervals of 1–5, it is necessary to multiply the expression in Formula (3) by 20, whereby the result is expressed in percentage points.

$$P_j = 20 \sum_{k=1}^{l} MP_k w_k \tag{3}$$

where P_j = the jth variable of the critical infrastructure element's resilience [%]; MP_k = the kth measurable item of the critical infrastructure element's resilience [number of points]; w_k = the kth normalized weight of the kth measurable item of the critical infrastructure element's resilience at interval ⟨0; 1⟩; l = the total number of measurable items in the jth variable.

Calculation of formulas (1)–(3) uses linear aggregation of weighted values. This method of calculation may be subject to a number of problems. Particularly significant is the implicit possibility of substitution, i.e., the possibility of offsetting a lower value of one variable by a higher value of the second variable. This presents a problem, especially if the result should be compared, for example, to different elements. However, the current version of the methodology does not allow for this use. The endeavor to "game" the system is technically possible but makes practically no sense, because nothing compels the operator to use this particular system of evaluation.

The advantage of linear aggregation is the ease of understanding and relative simplicity of interpreting the results, which were the main reasons for choosing this method of calculation by the authoring team of the methodology. However, if in the future, the problem of comparability across elements were solved, then formulas (1)–(3) would need to be revised using non-compensatory methods (e.g., [32,33]).

Table 3 – Comparative table for assessing the resilience of the element and its components and variables.

The resilience level of the element R, components K and variables P	
High level of resilience	85–100%
Acceptable level of resilience	69–84%
Low level of resilience	53–68%
Unsatisfactory level of resilience	37–52%
Critical level of resilience	≤36%

In view of the above-mentioned relationships (Formulas (1)–(3)), the aggregate formula for calculating the level of the critical infrastructure element's resilience can be defined as follows (Formula (4)):

$$R = \frac{1}{n} \sum_{i=1}^{n} \sum_{j=1}^{m} 20 v_j \sum_{k=1}^{l} MP_k w_k \tag{4}$$

The values of individual variables and components are calculated using the assessment forms of robustness, recoverability and adaptability. The resulting level of the element's resilience is determined and the final assessment completed in the last assessment form.

The final activity of the procedure to assess the critical infrastructure element's resilience consists of assessing the resilience level, identifying any weak points and proposing measures to strengthen the element's resilience (*Activity 9*). The level of resilience may be assessed at the level of the element (i.e. complex assessment), the component (i.e. partial assessment) or the variable (i.e. elementary assessment). A comparative table is used to assess the level of resilience (see Table 3).

The division of the resilience acceptability levels in Table 3 is based on the failure mode, effects and criticality analysis [34] method, which uses multiple variables to determine the risk level, and is based on variations in their extreme values. Similarly, individual resilience levels have been determined, which take into account variations in extreme values (i.e., 1 and 5) for five variables:

- Critical level: 1,1,1,1,5 => Ø 1.8 => 36%
- Insufficient level: 1,1,1,5,5 => Ø 2.6 => 52%
- Low level: 1,1,5,5,5 => Ø 3.4 => 68%
- Acceptable level: 1,5,5,5,5 => Ø 4.2 => 84%
- High level: 5,5,5,5,5 => Ø 5.0 => 100%

The division of resilience acceptability into five grades of assessment is guided by an effort to motivate users to explore in more detail the composition of resilience, i.e., the retrospective decomposition of component resilience and variable ratings. In view of the fact that the methodology is not intended to serve for mutual comparison across elements, the authors consider the requirement for a weak consistency of assessment [35] to be sufficient.

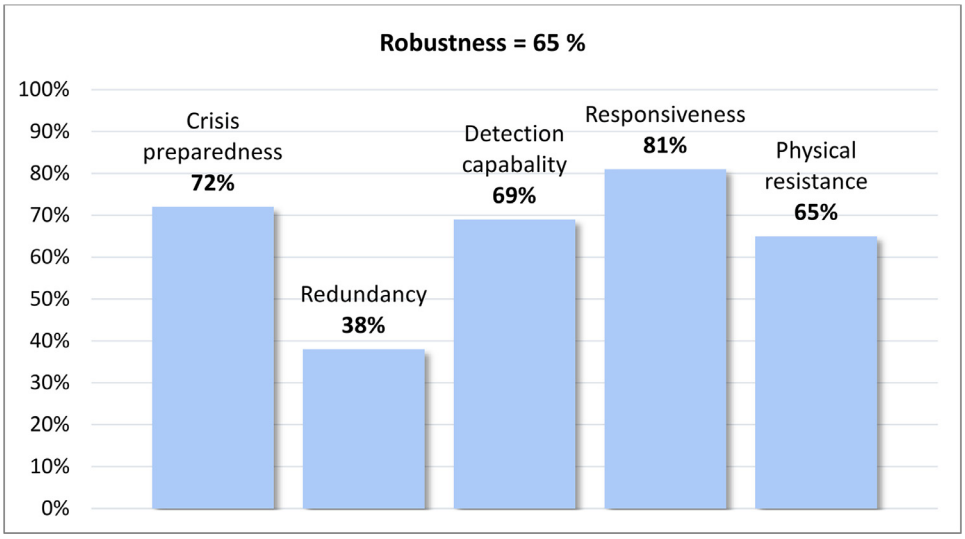

Fig. 6 – The robustness level of the critical infrastructure element.

The level of resilience R indicates the overall condition of the element (i.e. its ability to absorb the impacts of disruptive events and to recover its function to the original/required level of performance after the effects of a disruptive event have ended) and the condition of the organization (i.e. the ability of a critical infrastructure operator to prepare an element for the recurring effects of a previous disruptive event). The level of resilience K indicates the condition of individual components, while the level of resilience P indicates the condition of individual variables.

Where the resilience level reaches $\leq$ 68%, it will be necessary to identify the weak points through the decomposition of the resilience assessment results, which is to be done at the level of the affected measurable items. In cases where measurable items show a resilience point value of 3 and less, the affected areas of the assessed element will need to be revised and the process of their adjustment and recovery initiated.

The decomposition of the resilience assessment results will make it possible to propose measures aimed at strengthening the element's resilience. Resilience must always be strengthened at the lowest level, i.e. at the level of measurable items, as follows:

- High level of resilience (5): as the measurable items in this category show excellent parameters, there is no need to adopt any further measures.
- High level of resilience (4): the measurable items in this category show very good parameters which can still be improved upon, but such improvements are not necessary for the overall level of the element's resilience.
- Low level of resilience (3): the measurable items in this category show sufficient parameters, although their improvement would lead to substantial strengthening of the element's resilience.
- Unsatisfactory level of resilience (2): the measurable items in this category show very poor parameters which greatly reduce the resilience of the variable to which they belong.
- Critical level of resilience (1): the measurable items in this category are either absent or show critically low parameters. It is imperative that these items are fully revised and the process of their adjustment and restoration is initiated as soon as possible.

Table 4 – Normalized weights of variables determining the robustness of critical infrastructure elements based on the element's topology.

Variables	Point element weights	Areal element weights	Line element weights
Crisis preparedness	0.15	0.15	0.25
Redundancy	0.15	0.20	0.25
Detection capability	0.25	0.25	0.20
Responsiveness	0.20	0.25	0.15
Physical resistance	0.25	0.15	0.15
Σ	**1.00**	**1.00**	**1.00**

3.2. *Establishing the weights of variables and measurable items*

The v_j a w_k weights constitute an important part of the assessment (see Formulas (2) and (3)), as the weight values allow differentiation of the significance of individual components of the assessment. Following consultations held with the intended users of the method, the research team arrived at the conclusion that the weights should be derived separately for different types of critical infrastructure elements. See Table 4 for an example of normalized weights of variables determining the element's robustness.

The values were estimated based on the expert evaluation of assumed future users and by applying the paired comparison method. The values of the derived weights were

Table 5 – Description of the electricity critical infrastructure element being assessed.

Name of element	Control room of the distribution system operator
Sector/subsector:	Energy/electricity/distribution system
Topological structure:	Areal element:
Key technologies:	1. SCADA systems (a) Control system for operating the distribution system elements (b) Communication control system (c) Command system 2. Geographic information system
Number of distribution nodes:	740,000

Table 6 – Description of the threat against which the element was assessed.

Name of threat:	Cyber attack
Category of threat	Anthropogenic
Group of threats:	Cyber
Specification of threat:	SCADA system disruption

normalized so that their sum in the variable (w_k) and in the component (v_j) equalled 1 (Formula (5)).

$$\sum_{j=1}^{m} v_j = \sum_{k=1}^{l} w_k = 1 \tag{5}$$

By its very nature, the expert evaluation and scales derived from it will always be subjective to a certain extent. Given that intense research is still ongoing in this area, there is no widely accepted hierarchy of items, and so the assessment must be somewhat subjective. The use of such approaches in management is not unusual [36]. Specifications of weighting coefficients allow this subjectivity to be transparently collected in one place and admitted. If necessary, the weighting system can be revised in the future.

4. CIERA method case study

The initial verification of the method was done by analyzing the results of the realized case studies that were processed for the sectors of electricity (control room of the distribution system operator), transport (a railway station on an international track) and public health (a university hospital). The results were subsequently discussed with the operators of the elements being assessed and applied to adjusting the method further. The anonymous results of one of the assessments are presented below with a view to facilitating the interpretation of the use of the CIERA method.

For the purposes of the assessment, the control room of an undisclosed power distribution company was selected (*Activity 1*). This company operates in three regions, where it distributes electricity to nearly 740,000 customers (businesses and households).

Subsequently, the selected element was described (*Activity 2*) as to its structural and performance parameters and categorized within the structure of critical infrastructure. The element's structural parameters specify its topological structure and, in the case of areal elements, key technologies. The element's performance parameter with regard to the control room is the number of distribution nodes. These data are presented in Table 5.

The assessment of the resilience of this particular element was carried out with respect to seven selected threats (*Activity 3*). However, due to its extent, this subchapter includes only the assessment results concerning the element's resilience in connection with cyber-attacks. See Table 6 for a description of this threat (*Activity 4*).

The following part of the case study presents the assessment results with respect to the element's robustness, recoverability and adaptability. The first step was to assess the robustness of the element (*Activity 5*), which consisted of assessing the current condition (level) of its individual variables, i.e. the element's crisis preparedness, redundancy, detection capability, responsiveness and physical resistance. For the assessment results, see Fig. 7.

The next step was to assess the recoverability of the element (*Activity 6*), which consisted of assessing the current condition (level) of individual variables, i.e. material resources, financial resources, human resources and recovery processes. For the assessment results, see Fig. 8.

The element's adaptability was the last resilience component to be assessed (*Activity 7*). The assessment of the ele-

Table 7 – Identification of weak points in the resilience of the assessed element.

	Measurable items with an unsatisfactory level of resilience	Measurable items with a critical level of resilience
Robustness	1.1.1 CSIRT/Organization's security team	1.3.4 Incident reporting
Recoverability	–	–
Adaptability	3.1.1 Risk management level 3.1.4 Disruptive scenario specification 3.2.4 Management processes innovation	3.1.2 Risk assessment methodology 3.1.3 Safety standard implementation 3.2.1 Organizational structure 3.2.3 Management of organizational processes 3.2.7 Research and development

CIERA
Critical Infrastructure Elements Resilience Assessment

Critical Infrastructure Elements Resilience Assessment

Control room of the distribution SO — *Element name*

Cyber attack on the SCADA system — *Threat name*

2015-2019 RESILIENCE Critical Infrastructure

1. Assessment of Robustness

Number	Variables	Measurable items	Score [1-5]	Weight w_k	Variable $P_j = 20 \sum MP_k w_k$ [%]	Weight v_j	Component $K_i = \sum P_j v_j$ [%]
1.1.1	Crisis preparedness	CSIRT/security team in organisation	2	0,4	60 %	P = 0,15 A = 0,15 L = 0,25	83,5 %
1.1.2		Continuity planning	3	0,2			
1.1.3		Recovery planning	3	0,2			
1.1.4		Evaluation/audit of the security and risk analysis	5	0,2			
1.2.1	Redundancy	Backup data center	5	0,5	100 %	P = 0,15 A = 0,20 L = 0,25	
1.2.2		Backup control workplaces	5	0,2			
1.2.3		Available redundant capacity	5	0,3			
1.3.1	Detection capability	Auditing events in systems	4	0,15	76 %	P = 0,25 A = 0,25 L = 0,20	
1.3.2		IDS/IPS/SIEM system	3	0,15			
1.3.3		Firewall/demilitarized zone	5	0,4			
1.3.4		Incident reporting	1	0,15			
1.3.5		Asset monitoring	4	0,15			
1.4.1	Responsiveness	Activation of backup data center	5	0,4	88 %	P = 0,20 A = 0,25 L = 0,15	
1.4.2		Solving problems	4	0,6			
1.5.1	Physical resistance	Technical means	5	0,2	90 %	P = 0,25 A = 0,15 L = 0,15	
1.5.2		Protective measures	5	0,3			
1.5.3		System measures	4	0,5			

Fig. 7 – Assessment of the element's robustness with respect to cyber-attacks.
Legend: *P* = point element, *A* = areal element, *L* = line element.

ment's adaptability consisted of assessing the current condition (level) of individual variables, i.e. risk management and innovation, education and development processes. For the assessment results, see Fig. 9.

The core activity of the assessment was the calculation of the element's resilience (*Activity 8*). The resilience level of the critical infrastructure element was calculated as the arithmetic mean of the component values that determine it (see Formula (1)). For the assessment results, see Fig. 10.

The final activity of the procedure to assess the critical infrastructure element's resilience consisted of assessing the resilience level, identifying any weak points and proposing measures to strengthen the element's resilience (*Activity 9*). The level of resilience was assessed gradually based on comparative values (see Table 3) at three levels.

The lowest level at which resilience is assessed is the element level. In this regard, the element's resilience to cyber-attacks can be said to be 76.8%, which is considered an acceptable level of resilience.

This was followed by resilience assessment at the component level. The resilience of the element's robustness and recoverability is 83.5% and 88.3% respectively, which can be regarded as a high or near-high level of resilience. However, in terms of the element's adaptability, the value is 58.6%, which is a low, nearly unsatisfactory level. Since some variables of this component show very poor parameters, substantially reducing the element's resilience, it is essential that the relevant areas of the assessed element be revised.

The final level is the level of variables. In this case, the resilience of most of the variables is 69% or more, which is considered to be an acceptable level or resilience. Crisis Preparedness (60%) and Innovation Processes (60%) can be regarded as the weakest variables, while Risk Management is at a critical level of resilience with a mere 34% (see Table 3). It is important that the weak points in the element's resilience are subsequently identified with respect to these variables. This task involves identifying the measurable items that are at unsatisfactory or critical levels in the assessment (see Table 7).

Following the identification of weak points, it will be necessary to formulate a proposal for measures designed to strengthen the element's resilience. With respect to measurable items at an unsatisfactory level of resilience (point score 2), we recommend focusing especially on risk management, where the scenarios of individual disruptive events need to be elaborated further. Conversely, measurable items assessed to be at a critically low level of resilience (point score 1) are either entirely missing or show critically low parameters. This concerns particularly the area of incident reporting and activities related to the element's organizational resilience. It is imperative that these items are fully revised and the process of their adjustment and restoration is initiated as soon as possible.

CIERA
Critical Infrastructure Elements Resilience Assessment

Critical Infrastructure Elements Resilience Assessment

Control room of the distribution SO — *Element name*

Cyber attack on the SCADA system — *Threat name*

2015-2019 RESILIENCE Critical Infrastructure

2. Assessment of Recoverability

Number	Variables	Measurable items	Score [1-5]	Weight w_k	Variable $P_j = 20 \sum MP_k w_k$ [%]	Weight v_j	Component $K_i = \sum P_j v_j$ [%]
2.1.1	Material resources	Ability of the asset to recover its function	5	0,3	94 %	P = 0,2 A = 0,2 L = 0,3	88,3 %
2.1.2		Reparability of the assets key technology	5	0,2			
2.1.3		Availabilty of the spare parts at the time of need	5	0,1			
2.1.4		Replaceability of assets key technology	5	0,2			
2.1.5		Time horizon of repairing or replacing key technology	4	0,1			
2.1.6		Reliability criterion	3	0,1			
2.2.1	Financial resources	Allocation of the financial resources/reserves for recovery	5	0,3	100 %	P = 0,2 A = 0,2 L = 0,3	
2.2.2		Availability of financial resources/reserves in time of need	5	0,5			
2.2.3		Preparedness of financial resources/reserves in time of need	5	0,2			
2.3.1	Human resources	Availability of human resources with required qualification	4	0,25	85 %	P = 0,3 A = 0,3 L = 0,2	
2.3.2		Capacity of human resources	4	0,2			
2.3.3		Qualification of human resources	4	0,2			
2.3.4		Personal security	4	0,1			
2.3.5		Availability of human resources in time of need	5	0,25			
2.4.1	Recovery processes	Planning for function recovery	4	0,3	80 %	P = 0,3 A = 0,3 L = 0,2	
2.4.2		Process of function recovery	4	0,5			
2.4.3		Crisis preparedness of the recovery processes	4	0,2			

Fig. 8 – Assessment of the element's recoverability with respect to cyber-attacks.
Legend: *P* = point element, *A* = areal element, *L* = line element.

5. Conclusion

The CIERA quantitative method presented in this paper has been designed for Critical Infrastructure Elements Resilience Assessment. The method primarily relies on the complex assessment of the robustness, recoverability and adaptability of elements in technically oriented sectors with respect to disruptive events of naturogenic, technogenic and anthropogenic origin. It takes into account the functional, structural and performance parameters of the elements being assessed, while facilitating the identification of the element's weak points. When incorporated into the risk management system, this type of information will prove useful in proposing appropriate measures aimed at strengthening the element's resilience. The benefit of this method is that it allows for the assessment to be carried out at the level of the particular elements, for element resilience is the factor determining the resilience of higher critical infrastructure subsystems formed by these elements.

The CIERA method has been designed to assess separate elements in a critical infrastructure system. In terms of assessing critical infrastructure as a whole, it constitutes the first step in assessing the resilience of individual subsystems, with due consideration given to the determined limiting conditions. This step can therefore be followed by a comparative evaluation (or ranking) of elements within the operator's infrastructure. While the method can aid this step in the process by providing some useful data, it will not solve it by itself. For direct comparison, it will be necessary to resolve the issue of overcoming the differences between the various types of elements in the operated infrastructures (i.e. point, areal, line infrastructures), or to aggregate the assessments into directly comparable units.

The case study presented in the final part of the paper provides an example of the practical application of the CIERA method. The critical infrastructure element being assessed is the control room of an undisclosed power distribution company. As the assessment results show, the weakest area is the element's organizational resilience, especially with regard to its static organizational structure, insufficient management of organizational processes and very low investment in research and development of protection mechanisms against cyber-attacks. Concerning the element's technical resilience, the assessment revealed the absence of an incident reporting process, an inadequate risk management policy and insufficient specification of disruptive event scenarios.

CIERA
Critical Infrastructure Elements Resilience Assessment

Critical Infrastructure Elements Resilience Assessment

Control room of the distribution SO — *Element name*

Cyber attack on the SCADA system — *Threat name*

2015-2019 RESILIENCE Critical Infrastructure

3. Assessment of Adaptability

Number	Variables	Measurable items	Score [1-5]	Weight w_k	Variable $P_j = 20 \sum MP_k w_k$ [%]	Weight v_j	Component $K_i = \sum P_j v_j$ [%]
3.1.1	Risk management	Risk management level	2	0,4	34 %	0,4	58,6 %
3.1.2		Risk assessment methodology	1	0,2			
3.1.3		Implementation of security standards	1	0,1			
3.1.4		Level of scenarios for disruptive events	2	0,3			
3.2.1	Innovation processes	Organizational structure	1	0,1	60 %	0,3	
3.2.2		Implementation of management systems	4	0,1			
3.2.3		Management of organizational processes	1	0,1			
3.2.4		Innovation of management processes	2	0,1			
3.2.5		Technology innovation	4	0,2			
3.2.6		Innovation of security measures	4	0,2			
3.2.7		Research and development	1	0,1			
3.2.8		Innovation investment	5	0,1			
3.3.1	Education and development processes	Types of education provided or permitted by organization	5	0,2	90 %	0,3	
3.3.2		Scope of education	5	0,3			
3.3.3		Training to deal with the disruptive event	4	0,3			
3.3.4		Evaluation of the training's effectivity	4	0,2			

Fig. 9 – Assessment of the element's adaptability with respect to cyber-attacks.

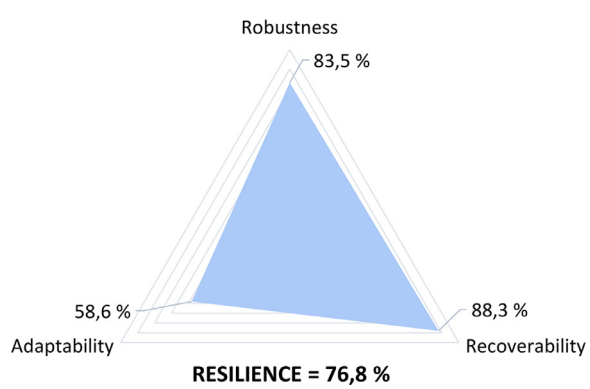

Fig. 10 – The resilience level of the assessed element.

Funding

The article was supported by the Ministry of the Interior of the Czech Republic [grant number VI20152019049].

REFERENCES

[1] President's Commission on Critical Infrastructure Protection. Critical Foundations: Protecting America's Infrastructures, The White House, Washington, DC, 1997.

[2] A. Sarri, K. Moulinos, Stocktaking, Analysis and Recommendations on the Protection of CIIs, ENISA, Heraklion, 2015. doi:10.2824/534303.

[3] Act No. 240/2000 Coll. on Crisis Management and on amendments of certain acts (Crisis Act) as amended.

[4] National Infrastructure Advisory Council. Critical Infrastructure Resilience Final Report and Recommendations, U.S. Department of Homeland Security, Washington, DC, 2009.

[5] Presidential Policy Directive (PPD-21). Critical Infrastructure Security and Resilience, The White House, Washington, DC, 2013.

[6] F. Petit, G. Bassett, R. Black, W. Buehring, M. Collins, D. Dickinson, R. Fisher, R. Haffenden, A. Huttenga, M. Klett, J. Phillips, M. Thomas, S. Veselka, K. Wallace, R. Whitfield, J. Peerenboom, Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience, Argonne National Laboratory, Chicago, IL, 2013.

[7] T. Prior, Measuring Critical Infrastructure Resilience: Possible Indicators (Risk and Resilience Report 9), Eidgenössische Technische Hochschule, Zurich, 2015.

[8] G. Bertocchi, S. Bologna, G. Carducci, L. Carrozzi, S. Cavallini, A. Lazari, G. Oliva, A. Traballesi, Guidelines for Critical Infrastructure Resilience Evaluation, Italian Association of Critical Infrastructures' Experts, Roma, 2016.

[9] C. Nan, G. Sansavini, A quantitative method for assessing resilience of interdependent infrastructures, Reliability Engineering and System Safety 157 (2017) 35-53. doi:10.1016/j.ress.2016.08.013.

[10] A. Jovanović, P. Klimek, A. Choudhary, N. Schmid, I. Linkov, K. Øien, M. Vollmer, Analysis of Existing Assessment Resilience Approaches, Indicators and Data Sources, Stuttgart, 2018.

[11] B. Cai, M. Xie, Y. Liu, Y. Liu, Q. Feng, Availability-based engineering resilience metric and its corresponding evaluation methodology, Reliability Engineering & System Safety 172 (2018) 216-224. doi:10.1016/j.ress.2017.12.021.
[12] I. Eusgeld, C. Nan, S. Dietz, "System-of-systems" approach for interdependent critical infrastructures, Reliability Engineering and System Safety 96:6 (2011) 679-686. doi:10.1016/j.ress.2010.12.010.
[13] D. Rehak, J. Markuci, M. Hromada, K. Barcova, Quantitative Evaluation of the Synergistic Effects of Failures in a Critical Infrastructure System, International Journal of Critical Infrastructure Protection 14 (2016) 3-17. doi:10.1016/j.ijcip.2016.06.002.
[14] L. Labaka, J. Hernantes, J.M. Sarriegi, A framework to improve the resilience of critical infrastructures, International Journal of Disaster Resilience in the Built Environment 6:4 (2015) 409-423.
[15] Government of Canada. Action Plan for Critical Infrastructure (2014-2017), Public Safety Canada, Ottawa, 2014.
[16] L. Dueñas-Osorio, J.I. Craig, B.J. Goodno, Seismic response of critical interdependent networks, Earthquake Engineering & Structural Dynamics 36:2 (2007) 285-306. doi:10.1002/eqe.626.
[17] R. Guidotti, H. Chmielewski, V. Unnikrishnan, P. Gardoni, T. McAllister, J. van de Lindt, Modeling the resilience of critical infrastructure: The role of network dependencies, Sustainable and Resilient Infrastructure 1:3–4 (2016) 153-168. doi:10.1080/23789689.2016.1254999.
[18] X. He, E.J. Cha, Modeling the damage and recovery of interdependent critical infrastructure systems from natural hazards, Reliability Engineering & System Safety 177 (2018) 162-175. doi:10.1016/j.ress.2018.04.029.
[19] X. He, E.J. Cha, Modeling the damage and recovery of interdependent civil infrastructure network using Dynamic Integrated Network model, Sustainable and Resilient Infrastructure (2018) 1-16. doi:10.1080/23789689.2018.1448662.
[20] D. Rehak, P. Senovsky, S. Slivkova, Resilience of Critical Infrastructure Elements and its Main Factors, Systems 6:2 (2018) 21. doi:10.3390/systems6020021.
[21] C.S. Holling, Resilience and Stability of Ecological Systems, Annual Review of Ecology and Systematics 4 (1973) 1-23. doi:10.1146/annurev.es.04.110173.000245.
[22] D. Rehak, S. Slivkova, V. Brabcova, Evaluation the resilience of critical infrastructure subsystems, in: M. Cepin, R. Bris (Eds.), Safety and Reliability – Theory and Application, CRC Press, Boca Raton, FL, 2017, pp. 955-962.
[23] D. Rehak, M. Hromada, Failures in a Critical Infrastructure System, in: T. Nakamura (Ed.), System of System Failures, IntechOpen, London, 2018, pp. 75-93. doi:10.5772/intechopen.70446.
[24] M. Hromada, L. Lukas, M. Matejdes, J. Valouch, L. Necesal, R. Richter, F. Kovarik, System and Method of Assessing Critical Infrastructure Resilience, Association of Fire and Safety Engineering, Ostrava, 2013. (in Czech).
[25] IRDR DATA Project Working Group, Peril Classification and Hazard Glossary, Integrated Research on Disaster Risk IPO, Beijing, 2014.
[26] S.M. Rinaldi, J.P. Peerenboom, T.K. Kelly, Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies, IEEE Control Systems Magazine 21:6 (2001) 11-25. doi:10.1109/37.969131.
[27] J.L. Carlson, R.A. Haffenden, G.W. Bassett, W.A. Buehring, M.J. Collins III, S.M. Folga, F.D. Petit, J.A. Phillips, D.R. Verner, R.G. Whitfield, Resilience: Theory and Application, Argonne National Laboratory, Lemont, IL, 2012. doi:10.2172/1044521.
[28] C. Béné, R.G. Wood, A. Newsham, M. Davies, Resilience: New Utopia or New Tyranny? Reflection about the Potentials and Limits of the Concept of Resilience in Relation to Vulnerability Reduction Programmes, IDS Working Papers 405 (2012) 1-61. doi:10.1111/j.2040-0209.2012.00405.x.
[29] IEC 31010, Risk Management–Risk Assessment Techniques, International Electrotechnical Commission, Geneva, 2009.
[30] M. Hromada, Cascade and synergy effect modelling of interrelated critical infrastructure sub-sectors, VSB – Technical University of Ostrava, Ostrava, 2016. (in Czech).
[31] V. Brabcova, S. Slivkova, D. Rehak, F. Toseroni, J. Havko, Assessing the Cascading Effect of Energy and Transport Critical Infrastructure Elements: Case Study, Communications – Scientific Letters of the University of Žilina 20:2 (2018) 8-15.
[32] Handbook on constructing composite indicators: Methodology and user guide, Organisation for Economic Co-operation and Development, Paris, 2008.
[33] G. Munda, M. Nardo, Non-Compensatory/NonLinear Indexes for Ranking Countries: A Defensible Setting, Applied Economics 41:12 (2009) 1513-1523. doi:10.1080/00036840601019364.
[34] IEC 60812, Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA), International Electrotechnical Commission, Geneva, 2006.
[35] L.A. Cox, What's Wrong with Risk Matrices? Risk Analysis 28:2 (2008) 497-512. doi:10.1111/j.1539-6924.2008.01030.x.
[36] M. Grabinski, Management Methods and Tools, Gabler, Wiesbaden, 2007. doi:10.1007/978-3-8349-9295-6.